

U.S. Department of Energy
Cyber Security Program

REMOTE ACCESS
GUIDANCE



January 2007

*This Guidance document was
developed and issued outside of the
Departmental Directives Program.*

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides direction and defines minimum requirements for security of remote access to DOE and contractor information technology systems (i.e., accessing an information system [at the system or application level] from outside the system's accreditation boundary) in accordance with applicable Departmental and Federal information technology security laws and regulations.

The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

This Guidance is provided to Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-4, *National Security Systems Controls Manual*, in their Program Cyber Security Plans (PCSPs).

In addition, this Guidance provides a risk-based approach to defining remote access programs and policies in the PCSPs. Consistent with law and policy, Senior DOE Management organizations and their operating units must use a documented risk-based approach to make informed decisions regarding the use of remote access, implementing necessary security controls, and determining the acceptable level of residual risk. This risk-based approach must be consistent with the principles and guidelines DOE CIO Guidance CS- 3, *Risk Management Guidance*.

3. CANCELLATIONS.

None.

4. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to Which DOE CIO Guidance CS-24 is Applicable*.

Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their

operating units and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.
- c. Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provide additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM)*; the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

- a. Senior DOE Management PCSPs must define policies, processes, and procedures for allowing access to accredited systems from outside of the accreditation boundary (remote access¹) to include at least the following:
 - (1) Policies and processes governing the conditions under which remote access can be granted.
 - (2) Policies requiring Memoranda of Agreement (MOAs) and Interconnection Security Agreements (ISAs) governing operation and communication among systems participating in remote access. See DOE CIO Guidance CS-5, *Interconnection Agreements*, for more information on the criteria for these agreements.
- b. Program Cyber Security Plan. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE Manual 205.1-4, *National Security Systems Controls Manual*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement remote access policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs. Senior DOE Management PCSPs are to require operating units to define and document the following:
 - (1) Processes and procedures for granting and maintaining remote access privileges that include the following principles.
 - (a) Remote access user is initially granted and annually revalidated based on authorized business needs, including scientific and other collaborative activities.
 - (b) Remote user access will be based on the concept of least privilege (i.e., remote access must be limited to the minimum privileges required).
 - i. General user: access to only general services on the system for which remote access is authorized.

¹ The definition of remote access used in this Guidance differs from that used by the Office of Management and Budget (OMB) in its guidance related to Personally Identifiable Information (PII). Please refer to OMB M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, for more information.

- ii. Privileged user: limited access to services or files (e.g., special read, write, delete, operator, system recovery, etc.) on the system allowing remote access.
 - iii. Administrator: access to services or files (e.g., system administration, special read, write, delete, configuration change privileges, operator, system recovery, etc.) on the system allowing remote access.
- (2) Develop or define and describe the following controls.
 - (a) Procedures to ensure the conduct of periodic and random security tests/evaluations of controls on remote access systems.
 - (b) Rules of behavior and operations and consequences for violating remote access policy and procedures, including the prohibition of entering any classified information on any remote computing resource not approved for such information.
 - (c) Processes for system owner and data custodian approval of remote access.
 - (d) Controls and safeguards for Government-issued cryptographic keys, authentication tokens, passwords, on all equipment used for remote access.
 - (e) Procedures for obtaining user acknowledgement and understanding of minimum requirements and rules of behavior for remote access. These procedures should include user signature on a User Responsibility Statement that includes those requirements and rules of behavior.
 - (f) Processes that ensure that the minimum requirements for operating system and application software are determined for all remote systems.
 - (g) Processes to ensure that systems may be remotely accessed only from other accredited systems with the same confidentiality impact/Information Group (e.g., unclassified system being accessed is accredited for [Confidentiality, Moderate] and the remote system is accredited for [Confidentiality, Moderate]) or Boundary Protection Services and automated tools (e.g., firewalls, virtual private networks, encryption, controlled interfaces, etc.) are provided to manage remote access among accredited systems as described in the joint ISA.
 - (h) Acceptable types of personal identification for remote access.
 - (i) Clear-text, reusable passwords for remote access are prohibited. Legacy systems that use clear text passwords [see paragraph 5.b.(1) and 5.b.(3)]

in DOE CIO Guidance CS-12, *Password Management*] are prohibited from participating in remote access.

- (j) Privileged users and administrators are to use two-factor authentication and utilize a trusted path capability (i.e. Virtual Private Network (VPN), Protected Transmission System (PTS), etc.) for remote access initial sign-on/ logon.
- (k) General users accessing National Security Systems or unclassified systems containing information for which confidentiality impact is Moderate or High are to use two-factor authentication and a trusted path (i.e., VPN, PTS, transmission media under DOE physical control, etc.) for initial sign-on/ logon.
- (l) An inactivity time-out function is in place on all systems allowing remote access. Re-authentication of remote users is required for unclassified systems of Security Category Moderate or High after a period of inactivity of no greater than 30 minutes and all National Security Systems after a period of inactivity of no greater than 15 minutes.
- (m) Documentation of remote access.
 - i. When implementation or modification to remote access causes a significant change in the level of risk, the System Security Plan (SSP) must be updated to reflect the increased risk and risk mitigation techniques; re-accreditation is required.
 - ii. When modification to an existing system is made to allow remote access, threat statements, system risk assessments, and the SSP must be reviewed and updated, as needed, before incorporating remote access capabilities into a system, and re-accreditation is required.

7. CRITERIA UNIQUE TO NATIONAL SECURITY SYSTEMS.

Remote access to any National Security System is authorized only via a DOE approved trusted communications path as required by DOE M 205.1-4. Only personnel with the access authorization, Need-to-Know, and training in system security are to access National Security Systems.

8. REFERENCES.

References are listed in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

9. DEFINITIONS.

Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

Remote Access. Access to any Information system from outside the accreditation boundary of the information system.

10. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO GUIDANCE CS-24 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration